

EXHIBIT “A”

Supreme Court of Pennsylvania

Court of Common Pleas

Civil Cover Sheet

Lackawanna

County

For Prothonotary Use Only:

Docket No:

23CV238

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

Commencement of Action:

- ☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:

JANE DOE, ET AL.

Lead Defendant's Name:

SCRANTON QUINCY HOSPITAL COMPANY, LLC

Are money damages requested? ☒ Yes ☐ NoDollar Amount Requested: ☐ within arbitration limits
(check one) ☐ outside arbitration limitsIs this a Class Action Suit? ☒ Yes ☐ NoIs this an MDJ Appeal? ☐ Yes ☐ No

Name of Plaintiff/Appellant's Attorney: _____

☐ Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)

TORT (do not include Mass Tort)

- ☐ Intentional
☐ Malicious Prosecution
☐ Motor Vehicle
☐ Nuisance
☐ Premises Liability
☐ Product Liability (does not include mass tort)
☐ Slander/Libel/ Defamation
☒ Other:
 Pennsylvania Wire Tap Act
 18 Pa. C.S.A. § 5725

MASS TORT

- ☐ Asbestos
☐ Tobacco
☐ Toxic Tort - DES
☐ Toxic Tort - Implant
☐ Toxic Waste
☐ Other:

PROFESSIONAL LIABILITY

- ☐ Dental
☐ Legal
☐ Medical
☐ Other Professional:

CONTRACT (do not include Judgments)

- ☐ Buyer Plaintiff
☐ Debt Collection: Credit Card
☐ Debt Collection: Other

☐ Employment Dispute:
 Discrimination
☐ Employment Dispute: Other

☐ Other:

REAL PROPERTY

- ☐ Ejectment
☐ Eminent Domain/Condemnation
☐ Ground Rent
☐ Landlord/Tenant Dispute
☐ Mortgage Foreclosure: Residential
☐ Mortgage Foreclosure: Commercial
☐ Partition
☐ Quiet Title
☐ Other:

CIVIL APPEALS

- Administrative Agencies
☐ Board of Assessment
☐ Board of Elections
☐ Dept. of Transportation
☐ Statutory Appeals/Other

☐ Zoning Board
☐ Other:

MISCELLANEOUS

- ☐ Common Law/Statutory Arbitration
☐ Declaratory Judgment
☐ Mandamus
☐ Non-Domestic Relations
☐ Restraining Order
☐ Quo Warranto
☐ Replevin
☐ Other:

MAURI B. KELLY
LACKAWANNA COUNTY

NOTICE

2023 JAN 23 P 2:35

CLERK OF JUDICIAL

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

- (i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.
- (ii) actions for support, Rules 1910.1 et seq.
- (iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.
- (iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.
- (v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.
- (vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (c) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

IN THE COURT OF COMMON PLEAS OF
LACKAWANNA, COUNTY, PENNSYLVANIA

MAURI B. KELLY
LACKAWANNA COUNTY

JANE DOE,
INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

Plaintiff

v.

SCRANTON QUINCY HOSPITAL COM-
PANY LLC, SCRANTON HOSPITAL COM-
PANY, LLC, and WILKES-BARRE
HOSPITAL COMPANY, LLC, collectively
d/b/a COMMONWEALTH HEALTH

Defendant.

2023 JAN 23 P 2:35

CLERK OF JUDICIAL
RECORDS CIVIL DIVISION

23 CV 238

NOTICE

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you. YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

Lackawanna County Bar Association
233 Penn Avenue
Scranton, PA 18503
Telephone: (570) 969-9161

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hace falta asentar una comparecencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o notificacion. Ademas, la corte puede decidir a favor del demandante y requerir que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades u otros derechos importantes para usted. LLEVE ESTA DEMANDA A UN ABOGADO INMEDIATAMENTE, SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICIO, VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.

Lackawanna County Bar Association
233 Penn Avenue
Scranton, PA 18503
Telefono: ((570) 969-91

IN THE COURT OF COMMON PLEAS OF
LACKAWANNA, COUNTY, PENNSYLVANIA

JANE DOE,
INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

Plaintiff

v.

SCRANTON QUINCY HOSPITAL COM-
PANY LLC, SCRANTON HOSPITAL COM-
PANY, LLC, and WILKES-BARRE
HOSPITAL COMPANY, LLC, collectively
d/b/a COMMONWEALTH HEALTH

Defendant.

Docket No.

23 CV 038

MAURI B. KELLY
LACKAWANNA COUNTY
2023 JAN 23 P 2:35
CLERK OF JUDICIAL
RECORDS CIVIL DIVISION

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all other current Citizens of the Commonwealth of Pennsylvania similarly situated ("Class Members"), brings suit against Defendants Scranton Quincy Hospital Company, LLC, d/b/a Commonwealth Health and Moses Taylor Hospital, Scranton Hospital Company, LLC, d/b/a/ Commonwealth Health and Regional Hospital of Scranton, and Wilkes-Barre Hospital Company, LLC, d/b/a Commonwealth Health and Wilkes-Barre General Hospital (collectively "Commonwealth Health" or "Defendants"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

NATURE OF ACTION AND ALLEGATIONS

1. This case arises from Commonwealth Health's systematic violation of the medical privacy rights of its patients, exposing highly sensitive personal information to third parties without those patients' knowledge or consent.

2. Commonwealth Health assures visitors to its website that "We understand that your medical information is personal" and that "We are committed to protecting your medical information."¹ Contrary to these assurances, however, Commonwealth Health does not follow these policies, nor the law prohibiting such disclosures.

3. At all relevant times, Commonwealth Health disclosed information about its patients—including their status as patients, their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Facebook and other third parties without their patients' knowledge, authorization, or consent.

4. Commonwealth Health discloses this personal health information through the deployment of various digital marketing and automatic rerouting tools embedded on its websites that purposefully and intentionally redirect patients' personal health information to third parties who exploit that information for advertising purposes. Commonwealth Health's use of these rerouting tools causes its patients' personally identifiable information and the contents of its patients' communications exchanged with Commonwealth Health to be automatically redirected to third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, their rights as citizens of Pennsylvania, and both the express and implied promises of Commonwealth Health.

5. Commonwealth Health's conduct in disclosing such protected health information about its patients to Facebook and other third parties violates Pennsylvania law, including, but

¹ <https://www.commonwealthhealth.net/privacy-practices>

not limited to, 18 Pa. C.S. §§5701 *et seq* (the Wiretapping and Electronic Surveillance Control Act), 28 Pa. Code § 115.27 (Confidentiality of Medical Records), 49 Pa. Code § 16.61(a)(1) (Unprofessional and Immoral Conduct), and the duty of physician-patient confidentiality recognized in *Haddad v. Gopal*, 787 A.2d 975, 980 (Pa. Super. 2001).

6. On behalf of themselves and all similarly situated citizens in the Commonwealth of Pennsylvania, Plaintiff seeks an order enjoining Commonwealth Health from further unauthorized disclosures of her personal information; awarding statutory damages in the amount of \$1,000 per violation, attorney's fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

PARTIES TO THE ACTION

7. Defendant Scranton Quincy Hospital Company, LLC, d/b/a Commonwealth Health or Moses Taylor Hospital, is a Pennsylvania limited liability company with its principal place of business at 700 Quincy Ave., Scranton, PA 18150.

8. Defendant Scranton Hospital Company, LLC, d/b/a/ Commonwealth Health or Regional Hospital of Scranton, is a Pennsylvania limited liability company with its principal place of business at 746 Jefferson Ave., Scranton, PA 18150.

9. Defendant Wilkes-Barre Hospital Company, LLC, d/b/a Commonwealth Health or Wilkes-Barre General Hospital, is a Pennsylvania limited liability company with its principal place of business at 575 North River Street, Wilkes Barre, PA 18764.

10. Scranton Quincy Hospital Company, Scranton Hospital Company, and Wilkes-Barre General Hospital collectively do business throughout the state of Pennsylvania, including in Lackawanna County, as Commonwealth Health or Commonwealth Health System, and operate the website www.commonwealthhealth.net. Therefore, Scranton Quincy Hospital

Company, Scranton Hospital Company, and Wilkes-Barre General Hospital are collectively referred to as “Commonwealth Health” or “Defendants.”

11. Plaintiff, Jane Doe, is a Pennsylvania citizen residing in Lackawanna County, Pennsylvania, has been treated by Defendants’ physicians, and has been a patient of Moses Taylor Hospital and Regional Hospital of Scranton, and thus also a patient of Defendants.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Defendants pursuant to 42 Pa. Con. Stat. Ann. § 5322 and §5301 because Defendants regularly conduct business throughout the Commonwealth of Pennsylvania.

13. Venue is appropriate in Lackawanna County pursuant to Pa R.C.P. 2179(a)(2) because Defendants’ principal place of business is in Lackawanna County, and, upon information and belief, many of the acts or conduct giving rise to the cause of action asserted herein took place in Lackawanna County. Venue is also appropriate in this Court because Plaintiff, Jane Doe, resides in Lackawanna County.

FACTUAL BACKGROUND

A. Commonwealth Health routinely discloses the protected health information of their patients to third parties including Facebook.

14. Plaintiff Jane Doe is a patient of Commonwealth Health who has received treatment from Moses Taylor Hospital and Regional Hospital of Scranton.²

15. Pennsylvania courts have long recognized a “right to privacy” in the Constitution of the Commonwealth.³ The Pennsylvania Supreme Court, in fact, has held that the Pennsylvania

² <https://www.commonwealthhealth.net/hospitals>

³ See, e.g., *Pennsylvania State Educ. Ass’n v. Commonwealth Dep’t of Cmty. & Econ. Dev.*, 637 Pa. 337, 340, 148 A.3d 142, 144 (2016)

Constitution “provides even more rigorous and explicit protections for a person’s right to privacy than does the United States Constitution.”⁴

16. Medical patients in Pennsylvania such as Jane Doe have a legal interest in preserving the confidentiality of their communications with healthcare providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Commonwealth Health without their express written consent and authorization.⁵

17. As a health care provider, Commonwealth Health has fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

18. Commonwealth Health expressly and impliedly promises patients that they will maintain and protect the confidentiality of personally identifiable patient information and communications.

19. Commonwealth Health operates the website www.commonwealthhealth.net for patients.

20. Commonwealth Health’s website is designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues and treatment options, and joining support groups.

21. Notwithstanding patients’ reasonable expectations of privacy, Commonwealth Health’s legal duties of confidentiality, and Commonwealth Health’s express promises to the contrary, Commonwealth Health discloses the contents of patients’ communications and

⁴ See *id.* at 352-353 (internal quotations omitted).

⁵ See, e.g., *In re T.R.*, 557 Pa. 99, 105, 731 A.2d 1276, 1279 (1999) (recognizing constitutional “right to privacy” protects a citizen’s interest in “avoiding disclosure of personal matters.”); *In re “B”*, 482 Pa. 471, 486, 394 A.2d 419, 426 (1978) (barring disclosure of a patient’s “psychiatric records” under the constitutional right to privacy.)

protected healthcare information via automatic re-routing mechanisms embedded in the websites operated by Commonwealth Health without patients' knowledge, authorization, or consent.

B. The nature of Commonwealth Health's unauthorized disclosure of patients' health care information.

22. Commonwealth Health's disclosures of patients' personal healthcare information occur because Commonwealth Health intentionally deploys source code on the websites they operate, including <https://www.commonwealthhealth.net/>, that cause patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

23. By design, Facebook receives and records the exact contents of patient communications before the full response from Commonwealth Health to patients has been rendered on the screen of the patient's computer device and while the communication between Commonwealth Health and the patient remains ongoing.

24. Websites like those maintained by Commonwealth Health are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users via their web browsers.

25. The basic command that web browsers use to exchange data and user communications is called a GET request.⁶ For example, when a patient types "heart failure treatment" into the search box on Commonwealth Health's website and hits 'Enter,' the patient's web browser makes a connection with the server for Commonwealth Health's website and sends the following request: "GET search/q=heart+failure+treatment."

26. When a server receives a GET request, the information becomes appended to the next URL (or "Uniform Resource Locator") accessed by the user. For example, if a user enters

⁶ https://www.w3schools.com/tags/ref_httpmethods.asp

“respiratory problems” into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words “respiratory” and “problems” will be appended to the query string at the end of the URL of the webpage showing the search results.

27. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks ‘Enter’ or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

28. In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website’s responsive communication.

29. Unbeknownst to users, however, the website’s server may also redirect the user’s communications to third parties. Indeed, Google warns website developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users’ personally identifiable information being disclosed to Google.⁷ Typically, users are provided no notice that these disclosures are being made.

30. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

31. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user’s screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

⁷ <https://support.google.com/platformspolicy/answer/6156630?hl=en>

32. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a “tag manager” service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

33. These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world’s most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

34. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

C. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website.

35. Tracking pixels are lines of source code embedded in websites such as Commonwealth Health’s. Tracking pixels are particularly pernicious because they result in the disclosure of a variety of data that permits third parties to determine the unique personal identities of website visitors. While most users believe that the internet provides them with anonymity when, for example, they browse a hospital website for treatment information about a medical condition, that is not the case when the hospital website has embedded third party tracking devices, as Commonwealth Health has.

36. For example, an IP address is a numerical identifier that identifies each computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses

also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.⁸

37. Because of their uniquely identifying characteristics, IP address are considered personally identifiable information. Tracking pixels can (and typically do) collect website visitors' IP addresses.

38. Likewise, internet cookies also provide personally identifiable information. Cookies are small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Cookies are typically designed to acquire and record an individual internet user's communications and activities on websites and were developed by programmers to aid online advertising.

39. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

40. Cookies are considered personal identifiers, and tracking pixels can collect cookies from website visitors.

41. A third type of personally identifying information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

⁸ <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

42. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."⁹ The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.¹⁰ Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.¹¹

43. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.¹²

44. Browser-fingerprints are considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

45. A fourth kind of personally identifying information protected by law against disclosure are unique user identifiers (such as Facebook's "Facebook ID") that permit companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is an identifying number string that is connected to a user's Facebook profile.¹³ Anyone with access to a user's Facebook ID can locate a user's Facebook profile.¹⁴

⁹ <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹⁰ <https://pixelprivacy.com/resources/browser-fingerprinting/>

¹¹ <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹² <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/>

¹³ <https://www.facebook.com/help/211813265517027>

¹⁴ <https://smallseotools.com/find-facebook-id/>

46. Unique personal identifiers such as a person's Facebook are likewise capable of collection through pixel trackers.

D. Facebook's Business Model: Exploiting Users' Personal Data to Sell Advertising.

47. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

48. Facebook describes itself as a "real identity" platform.¹⁵ This means that users are permitted only one account and must share "the name they go by in everyday life."¹⁶ To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.¹⁷

49. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."¹⁸ Facebook has since evolved into one of the largest advertising companies in the world.¹⁹ Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.²⁰ This allows Facebook to make inferences about users based on their interests, behavior, and connections.²¹

50. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.²²

¹⁵ <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.>

¹⁶ <https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/>

¹⁷ <https://www.facebook.com/help/406644739431633>

¹⁸ <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>

¹⁹ <https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/>

²⁰ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

²¹ <https://www.facebook.com/business/ads/ad-targeting>

²² <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

51. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users' habits and interests.

52. Tracking information about users' habits and interests is a critical component of Facebook's business model because it is precisely this kind of information that allows Facebook to sell advertising to its customers. Facebook uses plug-ins and cookies to track users' browsing histories when they visit third-party websites. Facebook then compiles these browsing histories into personal profiles which are sold to advertisers to generate profits.

53. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

54. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook

offers advertisers 1.5 million people ‘whose activity on Facebook suggests that they’re more likely to engage with/distribute liberal political content’ and nearly seven million Facebook users who ‘prefer high-value goods in Mexico.’”²³ Aided by highly granular data used to target specific users, Facebook’s advertising segment quickly became Facebook’s most successful business unit, with millions of companies and individuals utilizing Facebook’s advertising services.

E. Facebook’s Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

55. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its “Like” and “Share” buttons (known as “social plug-ins”), and other methodologies, which it then uses to power its advertising business.

56. One of Facebook’s most powerful tools is called the “Meta Pixel.” Once a third-party like Commonwealth Health installs the Meta Pixel on its website, by default it begins sending user information to Facebook automatically.²⁴

57. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users’ activities as users navigate through a website.²⁵ Once activated, the Meta Pixel “tracks the people and type of actions they take.”²⁶ Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.²⁷ The Meta Pixel code works by sending Facebook a detailed log of a user’s interaction with a website

²³ <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>

²⁴ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

²⁵ <https://developers.facebook.com/docs/meta-pixel/>

²⁶ <https://www.facebook.com/business/goals/retargeting>

²⁷ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website or how far down a web page they scrolled.²⁸

58. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.²⁹

59. The information Meta Pixel captures and disclose to Facebook includes a referrer header (or “URL”), which includes significant information regarding the user’s browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.³⁰ When users enter a URL address into their web browser using the ‘http’ web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user’s browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

60. These search terms and the resulting URLs divulge a user’s personal interests, queries, and habits on third-party websites operating outside of Facebook’s own platform. In this manner, Facebook tracks users browsing histories on third-party websites, and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.³¹

61. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item

²⁸ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

²⁹ See, e.g., *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).

³⁰ *In re Facebook*, 956 F.3d at 596.

³¹ *In re Facebook*, 956 F.3d at 596.

to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifying information such as IP addresses, Facebook IDs, and other data that allow Facebook to identify the user. All this personally identifying data is available to be included each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

62. These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.³²

63. In exchange for installing its Meta Pixel, Facebook provides website owners like Commonwealth Health with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.³³ The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.³⁴

64. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

³² <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

³³ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

³⁴ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

65. Facebook touted Meta Pixel (which it originally called “Facebook Pixel”) as “a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website.”³⁵ According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites.³⁶

66. Facebook warns web developers that its Pixel is a personal identifier because it enables Facebook “to match your website visitors to their respective Facebook User accounts.”³⁷

67. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website’s persistent header) to reduce the chance of browsers or code from blocking Pixel’s execution and to ensure that visitors will be tracked.³⁸

68. Once Meta Pixel is installed on a business’s website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as “optional values” set by the business website.³⁹ Meta Pixel tracks this data regardless of whether a user is logged into Facebook. It is unclear how Facebook exploits the data collected from nonusers, but when asked by Congress about Facebook’s business practices, Mark Zuckerberg conceded that the company maintains “shadow profiles” on nonusers of Facebook.⁴⁰

69. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user’s internet browser, similar to how a “bug” or wiretap can capture audio information.

³⁵ <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>

³⁶ <https://www.oviond.com/understanding-the-facebook-pixel>

³⁷ <https://developers.facebook.com/docs/meta-pixel/get-started>

³⁸ <https://developers.facebook.com/docs/meta-pixel/get-started>

³⁹ <https://developers.facebook.com/docs/meta-pixel/>

⁴⁰ <https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/>

70. For example, the Meta Pixel is configured to automatically collect “HTTP Headers” and “Pixel-specific data.”⁴¹ HTTP headers collect data including “IP addresses, information about the web browser, page location, document, referrer and person using the website.”⁴² Pixel-specific data includes such data as the “Pixel ID and the Facebook Cookie.”⁴³

71. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user’s IP address, name, email, phone number, and specific Facebook ID, which identifies an individual’s Facebook user account. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user’s corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.⁴⁴

72. Facebook has a number of ways to uniquely identify the individuals whose data is being forwarded from third-party websites through the Meta Pixel.

73. If a user has a Facebook account, the user data collected is linked to the individual user’s Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

74. Alternatively, Facebook can link the data to a user’s Facebook account through the “Facebook Cookie.”⁴⁵ The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.⁴⁶

⁴¹ <https://developers.facebook.com/docs/meta-pixel/>

⁴² <https://developers.facebook.com/docs/meta-pixel/>

⁴³ <https://developers.facebook.com/docs/meta-pixel/>

⁴⁴ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

⁴⁵ <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>

⁴⁶ <https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/>

75. Facebook can also link user data to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls “Advanced Matching.” There are two forms of Advanced Matching: manual matching and automatic matching.⁴⁷ Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users’ Facebook accounts.

76. While the Meta Pixel tool “hashes” personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data.⁴⁸ In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.⁴⁹

77. Facebook also receives personally identifying information in the form of user’s unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user’s unique IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

78. Facebook also places cookies on visitors’ computers. It then uses these cookies to store information about each user. For example, the “c_user” cookie is a unique identifier that identifies a Facebook user’s ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

⁴⁷ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

⁴⁸ <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

⁴⁹ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

79. The data supplied by the `c_user` cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type `www.facebook.com/#`, with the `c_user` identifier in place of the “#.” For example, the `c_user` cookie for Mark Zuckerberg is 4. Logging into Facebook and typing `www.facebook.com/4` in the web browser retrieves Mark Zuckerberg’s Facebook page: `www.facebook.com/zuck`.

80. Similarly, the “`lu`” cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user’s browser makes to Facebook’s servers. Facebook employs similar cookies such as “`datr`,” “`fr`,” “`act`,” “`presence`,” “`spin`,” “`wd`,” “`xs`,” and “`fbp`” cookies to track users on websites across the internet.⁵⁰ These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.⁵¹

81. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user’s IP address. Facebook recognizes a visitor’s browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like `www.capitalhealth.org`, and target users with advertising based on their web activity.

⁵⁰ <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a#:~:text=browser%20session%20ends,-%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features>.

⁵¹ https://securehomes.esat.kulcuven.be/~gacar/fb_tracking/fb_plugins.pdf

D. Commonwealth Health has discretely embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' protected health information to Facebook.

82. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertisement efforts.

83. Facebook's intrusion into the personal data of the visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.⁵² Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

84. Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.⁵³ For example, websites can use this data to create "custom audiences" to target the specific Facebook user, as well as other Facebook users who match "custom audience's" criteria.⁵⁴ Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

⁵² <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

⁵³ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

⁵⁴ <https://developers.facebook.com/docs/marketing-api/reference/custom-audience/>

85. Meta Pixel is wildly popular and embedded on millions of websites. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.⁵⁵ Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for advertising purposes.⁵⁶

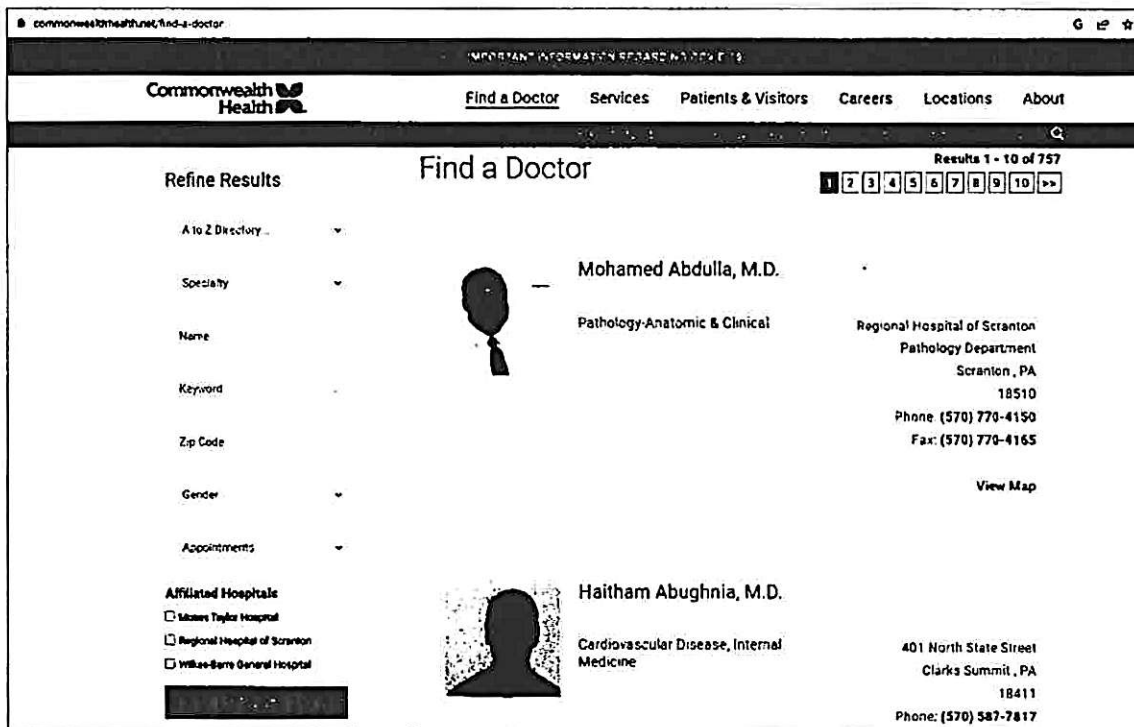
86. Shockingly, Meta Pixel is incorporated on many websites that are used to store and convey sensitive medical information, that by law must be kept private. Recently, investigative journalists have determined that Meta Pixel is embedded on the websites of many of the top hospitals in the United States.⁵⁷ This results in sensitive medical information being collected and then sent to Facebook when a user interacts with these hospital websites. For example, when a user on many of these hospital websites clicks on a “Schedule Online” button next to a doctor’s name, Meta Pixel sends the text of the button, the doctor’s name, and the search term (such as “cardiology”) used to find the doctor to Facebook. If the hospital’s website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

87. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, logout, or to create an appointment—Facebook code embedded on that page redirects the content of the patient’s communications to Facebook while the exchange of information between the patient and hospital is still occurring.

⁵⁵ <https://instapage.com/blog/meta-pixel>

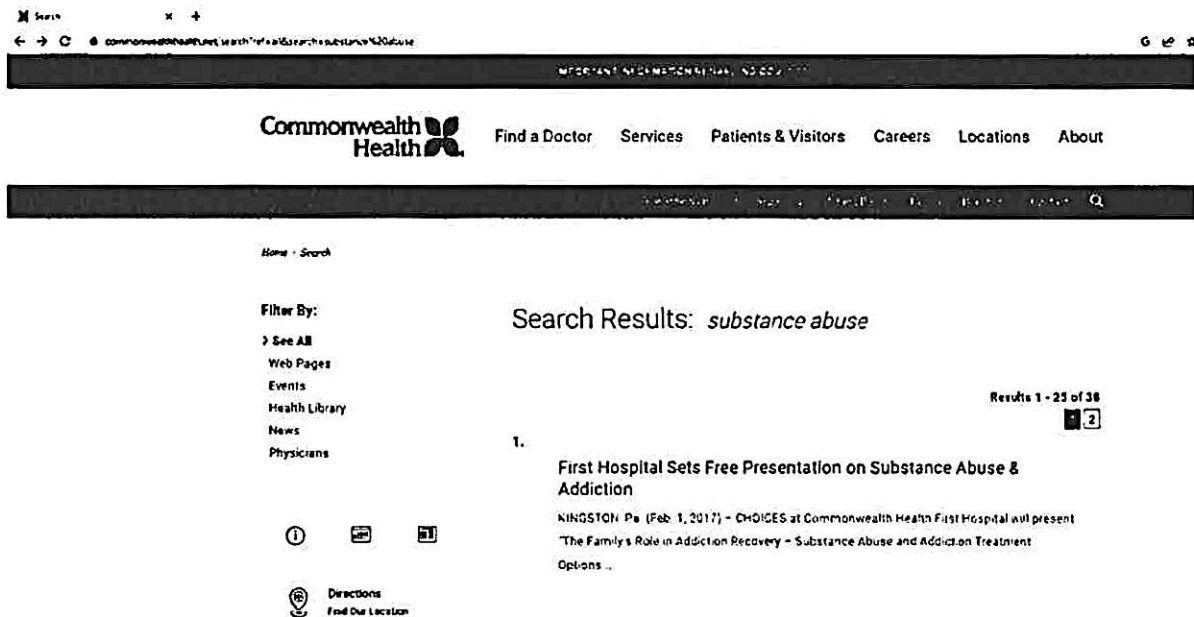
⁵⁶ <https://instapage.com/blog/meta-pixel>

⁵⁷ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>



91. All this data is disclosed to Facebook simultaneously in real time as patients transmit their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Commonwealth Health also discloses other personally identifying information to Facebook, such as patient IP addresses, cookie identifiers, browser-fingerprints, and device identifiers.

92. Commonwealth Health discloses such personally identifying information and sensitive medical information even when patients are searching for doctors on its websites to assist with them conditions such as substance abuse and addiction:



93. Commonwealth Health also discloses patient information from other sections of its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for "Services" offered by Commonwealth Health, communications made by patients using the website's Bill Pay/Financials function, and communications made when patients are researching specific medical conditions such as COVID-19. On information and belief, Commonwealth Health also makes similar disclosures to Facebook when patients click on "Log in" buttons of the password protected portions of its website.

94. As the above demonstrates, knowing what information a patient is reviewing on Commonwealth Health's website can reveal deeply personal and private information. For example, a simple search for "pregnant" on Commonwealth Health's website allows Meta Pixel to capture that search term and tell Facebook that the patient is likely pregnant. Indeed, Facebook might learn that the patient is pregnant before the patient's close family and friends. Likewise, most patients would not want it made public that they were seeking treatment for

substance abuse. But there is nothing visible on Commonwealth Health's website that would indicate to patients that, when they use Commonwealth Health's search function, their personally identifiable data and the precise content of their communications with Commonwealth Health are being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

95. The amount of data collected is significant. Via the Meta Pixel, when patients interact with its website, Commonwealth Health discloses a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient types a search term into the search bar on Commonwealth Health's website, the website returns links to information relevant to the search term. When patients then click these links, a communication is created that contains a GET request and a full-string detailed URL.

96. Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

97. The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Commonwealth Health's websites. The path identifies where a file

can be found on a website. For example, take <https://www.commonwealthhealth.net/find-a-doctor/amini-javid-md-9897>. Here, the “path” is [find-a-doctor/amini-javid-md-9897](https://www.commonwealthhealth.net/find-a-doctor/amini-javid-md-9897). Similarly, a patient reviewing information about the “Services” that Commonwealth Health offers patients such as “bariatric weight loss” will generate a URL with the path <https://www.commonwealthhealth.net/bariatric-weight-loss>.

98. Likewise, a query string provides a list of parameters. An example of a URL that provides a query string is <https://www.commonwealthhealth.net/search?ref=all&search=cancer>. The query string parameters in this search indicate that a search was done at the Commonwealth Health website for information about cancer. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider.

99. The contents of patients’ search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Commonwealth Health’s website. Worse, no matter how sensitive the area of the Commonwealth Health’s website that a patient reviews, the referral URL is acquired by Facebook along with cookies that precisely identify the patient.

100. The nature of the collected data is also important. Commonwealth Health’s unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient’s medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Commonwealth Health’s website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

101. Commonwealth Health also discloses the same kind of patient data described above to other third parties, including Google, Marketo, and LinkedIn via tracking software that

Commonwealth Health has installed on its website. As with the Facebook Meta Pixel, Commonwealth Health provides patients and prospective patients with no notice that Commonwealth Health is disclosing the contents of their communications to these third parties. Likewise, Commonwealth Health does not obtain consent from patients and prospective patients before forwarding their communications to these companies.

102. By compelling visitors to its websites to disclose personally identifying data and sensitive medical information to Facebook and other third parties, Commonwealth Health knowingly discloses information that allows Facebook and other advertisers to link its patients' Personal Health Information to their private identities and target them with advertising. Commonwealth Health intentionally shares the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

103. Commonwealth Health facilitated the disclosure of Plaintiff Jane Doe's Personal Health information, including sensitive medical information, to Facebook without her consent or authorization when he entered information on the websites that Commonwealth Health maintains. Plaintiff continued to have her privacy violated when Commonwealth Health permitted Facebook and other companies to send her targeted advertising related to her medical condition.

104. For example, Plaintiff Jane Doe has visited Commonwealth Health's website periodically at www.commonwealthhealth.net and entered data, including sensitive medical information, such as details about her medical condition and doctor. The information that Plaintiff Jane Doe transmitted included queries about potential physician(s) and treatment(s) for her medical condition. Plaintiff believed that her interactions with Commonwealth Health's website were private and would not be shared with anyone besides her healthcare providers.

Plaintiff was dismayed when she learned that Commonwealth Health's website had been capturing her Personal Health Information and disclosing that information to Facebook without her consent.

105. Commonwealth Health knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' Personal Health Information, including sensitive medical information and personally identifying data. Commonwealth Health was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Commonwealth Health made the decision to barter its patients' Personal Health Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Commonwealth Health and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

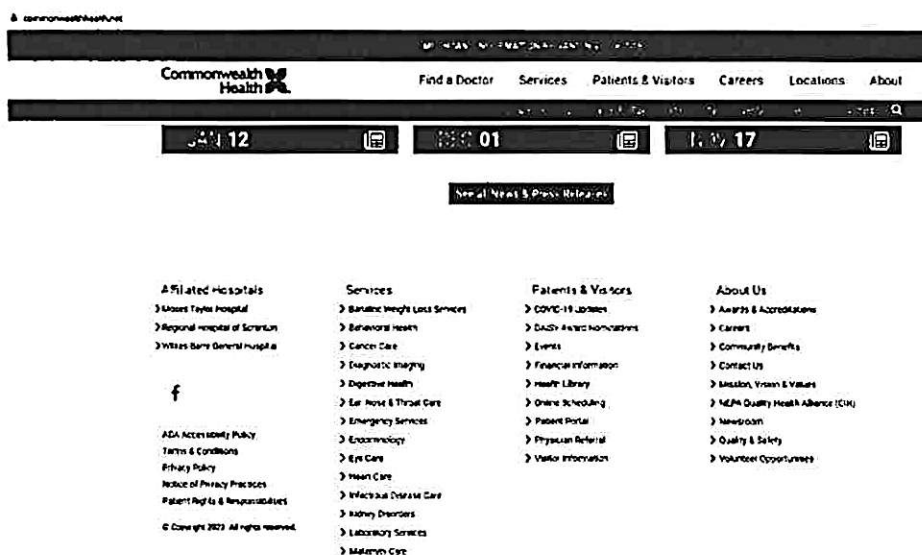
F. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

106. Plaintiff and Class Members had no idea when they interacted with Commonwealth Health's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is secretively and seamlessly integrated into Commonwealth Health's websites and is invisible to patients visiting those websites.

107. For example, when Plaintiff Jane Doe visited Commonwealth Health's website at www.commonwealthhealth.net there was no indication that the Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

108. Plaintiff and her fellow Class Members could not consent to Commonwealth Health's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

109. While Commonwealth Health purports to have a “Privacy Policy” and “Notice of Privacy Practices,” that policy and notice are effectively hidden from patients, buried at the bottom of Commonwealth Health’s homepage in type so small as to be unreadable to many visitors:



110. Even if a patient visiting Commonwealth Health’s website locates the Privacy Policy and Notice of Privacy Practices, nothing in those pages would be understood by any reasonable patient to mean that Commonwealth Health’s website routinely captures and exploits patients’ Personal Health Information, including by sharing that information with Facebook. To the contrary, neither Commonwealth Health’s Privacy Policy⁵⁸ nor its Notice of Privacy Practices⁵⁹ mention the Meta Pixel. Instead, Commonwealth Health’s Notice of Privacy Practices expressly states that “We understand that your medical information is personal. We are committed to protecting your medical information.”⁶⁰

⁵⁸ <https://www.commonwealthhealth.net/privacy-practices>

⁵⁹ <https://www.commonwealthhealth.net/hospital-privacy-policy>

⁶⁰ <https://www.commonwealthhealth.net/privacy-practices>

130. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers “should think of Facebook’s cost as [their] data and scrutinize the power it has to set its own price.”⁶⁷ This price is only increasing. According to Facebook’s own financial statements, the value of the average American’s data in advertising sales rose from \$19 to \$164 per year between 2013 and 2020.⁶⁸

131. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.⁶⁹

132. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,⁷⁰ and has paid teenagers and adults up to \$20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.⁷¹

133. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.⁷²

134. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Commonwealth Health has deprived Plaintiff and the Class

⁶⁷ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

⁶⁸ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

⁶⁹ <https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/>; *see also* <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁷⁰ <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app>

⁷¹ <https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>

⁷² <https://www.creditdonkey.com/best-apps-data-collection.html>; *see also* <https://www.monetha.io/blog/rewards/earn-money-from-your-data/>

Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff and the Class Member's property.

J. Commonwealth Health is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' protected health information.

135. In exchange for disclosing Personal Health Information about its patients, Commonwealth Health is compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

136. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

137. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

138. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Commonwealth Health loses the ability to control how that information is subsequently disseminated and exploited.

139. The monetization of the data being disclosed by Commonwealth Health, both by Commonwealth Health and Facebook, demonstrates the inherent value of the information being collected.

K. Facebook's history of egregious privacy violations.

140. Commonwealth Health knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

141. Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

142. In 2007, when Facebook launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

143. Two years later, Facebook made modifications to its Terms of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased using Facebook. The Terms of Service also failed to provide for any way for users to completely delete their accounts. Under immense public pressure, Facebook eventually returned to its prior Terms of Service.

144. In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when—in fact—the apps could access nearly all of a Facebook user's personal data. The resulting Consent Order prohibited Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the

extent to which Facebook makes user information available to third parties.⁷³

145. Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy rights by harvesting and storing Illinois' users' facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful act for \$650 million.⁷⁴

146. In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytics may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

147. Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.⁷⁵ Some companies were even able to read users' private messages.

148. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.⁷⁶ This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

⁷³ <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>

⁷⁴ A similar case is pending in Texas.

⁷⁵ <https://www.cnn.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html>

⁷⁶ <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>

149. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective ... at preventing the receipt of sensitive data."⁷⁷

150. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.⁷⁸ When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."⁷⁹

151. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use

⁷⁷ https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

⁷⁸ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁷⁹ <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"⁸⁰

152. These revelations were confirmed by an article published by the Markup on June 16, 2022, which found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.⁸¹

153. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' Personal Health Information to Facebook, Commonwealth Health did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

L. Commonwealth Health's failure to inform its patients that their Personal Health Information has been disclosed to Facebook or to take steps to halt the continued disclosure of such information is malicious, oppressive, and in reckless disregard of Plaintiff's and Class Members' rights.

154. Hospital systems, like other businesses, have a legal obligation to disclose data breaches to their customers. 73 Pa. C.S. § 2303.

155. After publication of the Markup's investigative article in June 2022, hospital systems around the United States began self-reporting data breaches arising from their installation of pixel technology on their websites.⁸²

⁸⁰ <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>

⁸¹ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

⁸² <https://www.scmagazine.com/analysis/breach/pixel-fallout-expands-community-health-informs-1-5m-of-unauthorized-disclosure>

156. For example, in August 2022, Novant Health informed approximately 1.3 million patients that their medical data was disclosed to Facebook due to the installation of the Facebook Meta Pixel on the hospital system's websites.⁸³ Novant Health's data breach announcement conceded that the Meta Pixel tool installed on its websites "allowed certain private information to be transmitted to Meta from the Novant Health website."⁸⁴ Novant Health further admitted that the information about its patients that was disclosed to Facebook included "an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes."⁸⁵

157. Likewise, in October 2022, Advocate Aurora Health informed approximately 3 million patients that their Personal Health Information had been disclosed to Facebook via the Meta Pixel installed on Advocate Aurora Health's website.⁸⁶

158. Advocate Aurora Health's data breach notification conceded that patient information had been transmitted to third parties including Facebook and Google when patients used the hospital system's website.⁸⁷

159. Advocate Aurora Health further admitted that a substantial amount of its patients' Personal Health Information has been shared with Facebook and Google including patients' "IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate

⁸³ <https://www.scmagazine.com/analysis/breach/1-3m-novant-health-patients-notified-of-unintended-disclosure-via-facebook-pixel>

⁸⁴ <https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident.aspx>

⁸⁵ <https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident.aspx>

⁸⁶ <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3>

⁸⁷ <https://www.advocateaurorahealth.org/>

Aurora Health location; information about your provider; [and] type of appointment or procedure.”⁸⁸ Even more troubling, Advocate Aurora Health admitted that “[w]e cannot confirm how vendors used the data they collected.”⁸⁹

160. Advocate Aurora Health claimed that, in conjunction with its data breach notice, the hospital system had “disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors.”⁹⁰ Advocate Aurora Health also promised its 3 million patients that the company had instituted an “enhanced, robust technology vetting process” to prevent such disclosures of its patients’ Personal Health Information in the future.⁹¹

161. Similarly, in October 2022, WakeMed notified more than 495,000 patients that their Personal Health Information had been transmitted to Facebook through the use of tracking pixels installed on its websites.⁹² In announcing this data breach, WakeMed admitted that the Facebook Meta Pixel tool had been installed on its website resulting in the transmission of patient information to Facebook.⁹³ WakeMed further admitted that “[d]epending on the user’s activity, the data that may have been transmitted to Facebook could have included information such as: email address, phone number, and other contact information; computer IP address; emergency contact information; information provided during online check-in, such as allergy or medication information; COVID vaccine status; and information about an upcoming

⁸⁸ <https://www.advocateaurorahealth.org/pixel-notification/faq>

⁸⁹ <https://www.advocateaurorahealth.org/pixel-notification/faq>

⁹⁰ <https://www.advocateaurorahealth.org/pixel-notification/faq>

⁹¹ <https://www.advocateaurorahealth.org/pixel-notification/faq>

⁹² <https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use>

⁹³ <https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident>

appointment, such as appointment type and date, physician selected, and button/menu selections.”⁹⁴

162. WakeMed also conceded that it had no idea what Facebook had done with the Personal Health Information that WakeMed had disclosed about its patients.⁹⁵ Like the other hospital systems who have come clean about their use of the Meta Pixel tool, WakeMed promised its patients that it had “proactively disabled Facebook’s pixel” and had “no plans to use it in the future without confirmation that the pixel no longer has the capacity to transmit potentially sensitive or identifiable information.”⁹⁶

163. In November 2022, the fallout from hospital systems’ use of the Meta Pixel tool expanded when Community Health Network informed 1.5 million of its patients that their personal health information had been routinely transmitted and disclosed to Facebook since at least April 2017.⁹⁷

164. In its data breach notice, Community Health admitted that it had “discovered through our investigation that the configuration of certain technologies allowed for a broader scope of information to be collected and transmitted to each corresponding third-party tracking technology vendor (e.g., Facebook and Google) than Community had ever intended.” Community Health further conceded that its use of the Meta Pixel and related third-party tracking technologies had resulted in surreptitiously recording and transmitting a wide range of patient engagements with its websites, including “includes scheduling an appointment online or

⁹⁴ <https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident>

⁹⁵ <https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident>

⁹⁶ <https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident>

⁹⁷ <https://healthitsecurity.com/news/community-health-network-notifies-1.5m-of-data-breach-stemming-from-tracking-tech>; see also <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

directly with a provider” and “seeking treatment at a Community or affiliated provider location.”⁹⁸

165. Community Health, like WakeMed, Novant, and Advocate Aurora Health, also promised its patients that it had disabled or removed the third-party tracking technologies that it had installed on its website and had instituted new “evaluation and management processes for all website technologies moving forward.”⁹⁹ Community Health, however, also conceded that it had no idea how Facebook or other third parties had exploited the patient Personal Health Information that had been disclosed to them via the pixel technology.

166. Unlike Community Health, WakeMed, Novant, Advocate Aurora Health, and other responsible hospital systems who have informed their patients of the serious privacy violations resulting from the installation of Facebook’s Meta Pixel tool on their websites, Commonwealth Health has done nothing. Indeed, not only has Commonwealth Health hidden these privacy violations from its patients, but Commonwealth Health continues to collect, transmit, and disclose its patients’ Personal Health Information to Facebook despite widespread knowledge in the health care community that such collection and disclosure of patient Personal Health Information is patently illegal and in violation of patient’s fundamental privacy rights.

167. As these data breach announcements demonstrate, there is widespread knowledge within the health care community that installation of the Meta Pixel tool on hospital websites results in the disclosure of patients’ Personal Health Information Facebook. There is also widespread recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy rights involved.

⁹⁸ <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

⁹⁹ <https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach>

168. Commonwealth Health's decision to hide its use of the Meta Pixel tool from its own patients and its refusal to remove such technologies from its websites even after learning that its patients' Personal Health Information was being routinely collected, transmitted, and exploited by Facebook is malicious, oppressive, and in reckless disregard of Plaintiffs' and Class Members' rights.

TOLLING, CONCEALMENT, AND ESTOPPEL

169. The applicable statutes of limitation have been tolled as a result of Commonwealth Health's knowing and active concealment and denial of the facts alleged herein.

170. Commonwealth Health seamlessly incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Commonwealth Health had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

171. Meta Pixel is purposefully designed and integrated in a way that makes it impossible to identify with the naked eye and its presence can only be discovered through means significantly more sophisticated than possessed by the average internet user.

172. Plaintiff and Class Members could not with due diligence have discovered the full scope of Commonwealth Health's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

173. Further, Plaintiff and Class Members were not on notice to look for the Meta Pixel, and Commonwealth Health's overt representations assured them that their personal information was being treated in a confidential manner.

174. The earliest that Plaintiff and Class Members, acting with due diligence, could have reasonably discovered this conduct would have been on June 16, 2022, following the release of the Markup's investigation.

175. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Commonwealth Health's illegal interception and disclosure of patients' Personal Health Information has continued unabated through the date of the filing of Plaintiff's Original Complaint. What's more, Commonwealth Health was under a duty to disclose the nature and significance of their data collection practices but did not do so. Commonwealth Health is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

176. Commonwealth Health's conduct violates the law, its duty of confidentiality, its express and implied promises, and Plaintiff's and Class Members' right to privacy.

177. Commonwealth Health's unlawful conduct has injured Plaintiff and Class Members.

178. Commonwealth Health's conduct is ongoing.

179. Plaintiff brings this action individually and as a class action against Commonwealth Health.

180. Plaintiff seeks class certification for the following proposed Class:

The Commonwealth Health Class: During the fullest period allowed by law, all current Pennsylvania citizens who are, or were, patients of Community Health (including, but not limited to, patients at Moses Taylor Hospital, Regional Hospital of Scranton, and Wilkes-Barre General Hospital), or any of its affiliates and who exchanged communications at Commonwealth Health's websites, including www.commonwealthhealth.net, and any other Commonwealth Health affiliated website.

181. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over

this action and members of their families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

182. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

183. Plaintiff seeks certification of this matter as a class action pursuant to Pennsylvania Rules of Civil Procedure § 1701 *et seq.*

184. **Numerosity:** While the exact number of Class Members is unknown to Plaintiff at this time, the Class, based on information and belief, consists of thousands of people dispersed throughout the Commonwealth of Pennsylvania, such that joinder of all members is impracticable. The exact number of Class Members can be determined by review of information maintained by Commonwealth Health.

185. **Commonality and Predominance:** There are questions of law and fact common to Class Members and which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

- a. Whether Commonwealth Health's acts and practices violated Plaintiff and Class Members' privacy rights;
- b. Whether Commonwealth Health's acts and practices violate 18 Pa. C.S. § 5703(1)-(3);
- c. Whether Commonwealth Health's acts and practices violate 28 Pa. Code § 115.27;
- d. Whether Commonwealth Health's acts and practices violate 49 Pa. Code § 16.61(a)(1);
- e. Whether Commonwealth Health's acts and practices violate the duty of doctor-

patient confidentiality recognized in *Haddad v. Gopal*, 787 A.2d 975, 980 (Pa. Super. 2001);

- f. Whether Commonwealth Health's acts and practices violate 55 Pa. Code § 5100.37;
- g. Whether Commonwealth Health's acts and practices violate 28 Pa. Code § 710.23;
- h. Whether Commonwealth Health's acts and practices violate 71 P.S. §§ 1690.108(b)(1) & (b)(2);
- i. Whether Commonwealth Health's acts and practices violate 50 P.S. § 7111;
- j. Whether Commonwealth Health knowingly allowed the surreptitious collection and disclosure of Plaintiff and Class Members' Personal Health Information to Facebook;
- k. Whether Commonwealth Health's acts and practices constitute a breach of fiduciary duty;
- l. Whether Commonwealth Health profited from disclosures of patient Personal Health Information to third parties including Facebook;
- m. Whether Commonwealth Health was unjustly enriched;
- n. Whether Commonwealth Health's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;
- o. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and
- p. Whether Plaintiff and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

186. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

187. Commonwealth Health engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

188. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members and Plaintiff have substantially the same interest in this matter as other Class Members. Plaintiff has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are patients of Commonwealth Health who used the websites set up by Commonwealth Health for patients and are victims of Commonwealth Health's respective unauthorized disclosures to third parties including Facebook. All claims of Plaintiff and Class Members are based on Commonwealth Health's wrongful conduct and unauthorized disclosures.

189. **Adequacy of Representation:** Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are coincident with, and not antagonistic to, those of other Class Members he seeks to represent. Plaintiff has no disabling conflicts with Class Members. Accordingly, Plaintiff is an adequate representative of the Class and, along with counsel, will fairly and adequately protect the interests of the Class and any Subclasses.

190. **Superiority:** A class action is the superior method for fair and efficient adjudication of the controversy. Although all Class Members have claims against Commonwealth Health, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. The damages, harm, and other financial detriment suffered individually by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Commonwealth Health, making it impractical for Class Members to individually seek redress for Commonwealth Health's wrongful conduct. Moreover,

serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. The prosecution of separate actions by individual Class Members could create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which could establish incompatible standards of conduct for Commonwealth Health or adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Commonwealth Health's misconduct will continue without proper remedy.

191. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable and direct notice can be provided from the records maintained by Commonwealth Health, electronically or by publication, the cost of which is properly imposed on Commonwealth Health.

192. For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action.

CAUSES OF ACTION

COUNT I

Violation of Wiretapping and Electronic Surveillance Control Act (WESCA), 18 Pa. C.S. § 5701 *et seq* (On Behalf of Plaintiff and the Class)

193. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

194. Plaintiff brings this claim on behalf of herself and all members of the Class.

195. All conditions precedent to this action have been performed or have occurred.

196. WESCA prohibits any person from:

- a. intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
- b. intentionally disclosing or endeavoring to disclose to any other person the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
- c. intentionally using or endeavoring to use the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication.

197. Any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation of WESCA “shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication.” 18 Pa. C.S. § 5725.

198. Commonwealth Health qualifies as a person under the WESCA. *See* 18 Pa. C.S. §5702.

199. Commonwealth Health has engaged in, and continues to engage in, intentionally intercepting, endeavoring to intercept, or procuring other person(s), including at least Facebook, to intercept or endeavor to intercept, the contents of alleged wire or electronic communications between Plaintiff or Class Members and Commonwealth Health.

200. In addition, or in the alternative, Commonwealth Health has engaged in, and continues to engage in, intentionally disclosing or endeavoring to disclose to other person(s), including at least Facebook, the contents of wire or electronic communications between Plaintiff or Class Members and Commonwealth Health, even though Commonwealth Health person knows, or at least has reason to know, that the information was obtained through the

interception of wire or electronic communications between Plaintiff or Class Members and Commonwealth Health.

201. In addition, or in the alternative, Commonwealth Health has engaged in, and continues to engage in, intentionally using or endeavoring to use the contents of wire or electronic communications between Plaintiff or Class Members and Commonwealth Health, even though Commonwealth Health person knows, or at least has reason to know, that the information was obtained through the interception of wire or electronic communications between Plaintiff or Class Members and Commonwealth Health.

202. All parties to the communications between Plaintiff or Class Members and Commonwealth Health alleged herein have not given prior consent to such interception because Plaintiff or Class Members, as parties to said communications, never gave such consent. *See* 18 Pa. C.S. §5704(4).

203. Plaintiff and Class Members reasonably expected that their Personal Health Information was not being intercepted, recorded, and disclosed to Facebook and other third parties.

204. No legitimate commercial purpose was served by Commonwealth Health's willful and intentional disclosure of Plaintiff's and Class Members' Personal Health Information to Facebook. Neither Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by Commonwealth Health to Facebook and other third parties. Nor could they have consented, given that Commonwealth Health never sought Plaintiff's or Class Members' consent, much less told visitors to its website that their every interaction was being recorded and transmitted to Facebook via the Meta Pixel tool.

205. Under the WESCA, aggrieved persons such as Plaintiff or Class Members are entitled to recover from Commonwealth Health:

- a. actual damages but not less than liquidated damages computed at the rate of \$100 per day for each violation or \$1,000, whichever is higher;
- b. punitive damages; and
- c. a reasonable attorney's fee and other litigation disbursements reasonably incurred."

206. In addition to statutory damages, Commonwealth Health's breach caused Plaintiff and Class Members the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Commonwealth Health eroded the essential confidential nature of the doctor-patient relationship;
- c. Commonwealth Health took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Commonwealth Health's duty to maintain confidentiality; and
- e. Commonwealth Health's actions diminished the value of Plaintiff and Class Members' personal information.

207. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Commonwealth Health in excess of \$1 million,

together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT II
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

208. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

209. Plaintiff bring this claim on behalf of herself and all members of the Class.

210. Pennsylvania law expressly recognizes that patients have a right to every consideration of privacy concerning their medical records. *See, e.g.*, 28 Pa. Code § 115.27; 49 Pa. Code § 16.61.

211. Commonwealth Health intentionally intruded upon the private concerns of Plaintiff and Class Members in their Personal Health Information.

212. Plaintiff and Class Members are current, former, or potential patients of Commonwealth Health.

213. Commonwealth Health owes Plaintiff and Class Members a duty of confidentiality.

214. Despite its duty not to disclose Personal Health Information, Commonwealth Health disclosed Personal Health Information of Plaintiff and Class Members without their knowledge, consent, or authorization.

215. The information disclosed included personally identifiable information, Plaintiff and Class Members' statuses as patients of Commonwealth Health, and the exact contents of communications exchanged between Plaintiff and/or Class Members with Commonwealth Health, including but not limited to information about treating doctors, potential doctors,

conditions, treatments, appointments, search terms, bill payment, and logins to Commonwealth Health's website.

216. Such disclosures constitute a substantial intrusion on the seclusion of Plaintiff's and Class Members' private concerns.

217. Commonwealth Health's intentional disclosure of patients' Personal Health Information to a third-party advertising company like Facebook without consent would be highly offensive to a reasonable person. Plaintiff and Class Members reasonably expected that their Personal Health Information would not be collected, used, and monetized by third party advertising companies

218. Commonwealth Health's disclosures of Personal Health Information of Plaintiffs and Class Members were highly offensive to a reasonable person at least because such disclosures violated expectations of privacy that have been established by the Pennsylvania Constitution, the Pennsylvania Patient's Bill of Rights, and established social norms. Privacy polls and studies show that Americans believe that one of the most important privacy rights is the need for an individual's affirmative consent before their personal data is collected, shared, or used.

219. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their Personal Health Information and were accordingly entitled to protection of this information against the acquisition and disclosure of their Personal Health Information by unreasonable means.

220. Commonwealth Health owed a duty to Plaintiff and Class Members to protect the confidentiality of their Personal Health Information and not to share such information with

Facebook for marketing purposes without the express written consent of Plaintiff and Class Members.

221. Commonwealth Health obtained Plaintiff's and Class Members' Personal Health Information by falsely promising that it would safeguard the confidentiality of that information and that it would never disclose such information to third parties for marketing purposes without written consent. The deceitful method through which Commonwealth Health obtained Plaintiff's and Class Member's Personal Health Information (i.e., lying to patients about how their Personal Health Information would be used) would be objectionable to a reasonable person.

222. The unauthorized acquisition, appropriation, and disclosure of Plaintiff's and Class Members' Personal Health Information would also be highly offensive to a reasonable person.

223. The intrusion was into subject matter that was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal Health Information to Commonwealth Health with the understanding that it would only be used for their medical treatment and that such information would be kept confidential and protected from disclosure to third parties. Plaintiff and Class Members reasonably believed that such information would be kept private and would not be shared with Facebook without their authorization so that Facebook could target them with advertising.

224. The disclosure of Plaintiff's and Class Members' Personal Health Information by Commonwealth Health constitutes an unreasonable intrusion upon Plaintiff's and Class Members' seclusion, as to both their persons, their private affairs, and private concerns of a kind that would be highly offensive to a reasonable person.

225. Commonwealth Health acted with a knowing mind when it intentionally disclosed Plaintiff and Class Members' Personal Health Information to Facebook. Commonwealth Health further invaded Plaintiff's and Class Members' privacy by failing to implement adequate data security measures, despite its obligations to protect patients' Personal Health Information.

226. Acting with knowledge, Commonwealth Health had notice and knew that its disclosure of Plaintiff's and Class Members' Personal Health Information would cause injury to Plaintiff and Class Members.

227. Given the nature of the Personal Health Information that Commonwealth Health disclosed to Facebook, such as patients' names, email addresses, phone numbers, information entered into forms, doctor's names, potential doctor's names, the search terms used to locate doctors (i.e. "Alzheimer's"), the condition selected from dropdown menus (i.e. "Heart Disease"), medications, and details about upcoming doctor's appointments, this kind of intrusion is both a substantial invasion of Plaintiff's and Class Members' privacy and would be (and in fact is) highly offensive to a reasonable person.

228. Commonwealth Health's breach caused Plaintiff and Class Members, at minimum, the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Commonwealth Health eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Commonwealth Health took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Commonwealth Health's duty to maintain the confidentiality of their Personal Health Information; and

- e. Commonwealth Health's actions diminished the value of Plaintiff and Class Members' personal information.

229. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

230. Plaintiff and Class Members have been damaged as a direct and proximate result of Commonwealth Health's invasion of their privacy and are entitled to seek just compensation, including monetary damages.

231. Plaintiff and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits made by Commonwealth Health as a result of its intrusions on Plaintiff and Class Members' privacy.

232. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Commonwealth Health's actions, which caused injury to Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Commonwealth Health from engaging in such conduct in the future.

233. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Commonwealth Health in excess of \$1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT III
Breach of Duty of Confidentiality
(On Behalf of Plaintiff and the Class)

234. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

235. Plaintiff brings this claim on behalf of herself and all members of the Class.

236. All conditions precedent to this action have been performed or occurred.

237. "Doctors have an obligation to their patients to keep communications . . . completely confidential." *Haddad v. Gopal*, 2001 PA Super 317, ¶ 5, 787 A.2d 975, 981 (Pa. Super. Ct. 2001).

238. As medical provider for Plaintiff and Class Members, Commonwealth Health owes Plaintiff and Class Members a fiduciary duty of confidentiality in the data and content of communications exchanged between Commonwealth Health and Plaintiff or Class Members.

239. Commonwealth Health breached its duty of confidentiality by disclosing Personal Health Information about Plaintiff and Class Members, including their status as patients, the content of their communications, and information about their doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment to Facebook and other third parties.

240. Commonwealth Health's breach caused Plaintiff and Class Members the following damages:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Commonwealth Health eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Commonwealth Health took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members'

knowledge, consent, or authorization and without sharing the benefit of such value;

- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Commonwealth Health's duty to maintain the confidentiality of their Personal Health Information; and
- f. Commonwealth Health's actions diminished the value of Plaintiff and Class Members' personal information.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Commonwealth Health in excess of \$1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

241. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

242. Plaintiff brings this claim on behalf of herself and all members of the Class.

243. Plaintiff and Class Members conferred a benefit on Commonwealth Health in the form of valuable sensitive medical information that Commonwealth Health collected from Plaintiff and Class Members under the guise of keeping this information private, and Commonwealth Health appreciated this benefit.

244. Commonwealth Health collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Commonwealth Health in the form of monetary compensation.

245. Plaintiff and the Class Members would not have used the Commonwealth Health's services, or would have paid less for those services, if they had known that Commonwealth Health would collect, use, and disclose this information to third parties.

246. Commonwealth Health unjustly retained those benefits at the expense of Plaintiff and Class Members because Commonwealth Health's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

247. The benefits that Commonwealth Health derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Commonwealth Health to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

248. Commonwealth Health should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Commonwealth Health received, and such other relief as the Court may deem just and proper.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Commonwealth Health in excess of \$1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT V
Breach of the Duty to Protect Electronic Data
(On Behalf of Plaintiff and the Class)

249. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

250. Plaintiff brings this claim on behalf of herself and all members of the Class.

251. As the Pennsylvania Supreme Court recognized in *Dittman v. UPMC*, 649 Pa. 496, 508-509 (Pa. 2018), businesses who collect and use sensitive personal information owe those whom they require to provide such information a duty to exercise reasonable care to protect that information from data breaches.

252. As a condition of receiving medical treatment, Commonwealth Health encouraged and required Plaintiff and Class Members to provide Personal Health Information when interacting with Commonwealth Health's websites. Commonwealth Health also affirmatively promised Plaintiff and Class Members that it would never disclose their Personal Health Information to third parties for marketing purposes without their express written authorization.

253. Commonwealth Health engaged in the affirmative act of collecting, storing, and maintaining Plaintiff and Class Members' sensitive personal and medical information on their internet-accessible websites computer systems. In doing so, Commonwealth Health was under a duty to Plaintiff and Class Members to protect them from the risk of having their Personal Health Information transmitted to third parties such as Facebook without their knowledge or express written consent.

254. Commonwealth Health collected, stored, maintained, and used Plaintiff and Class Members' Personal Health Information on its internet-accessible website and computer systems without use of adequate security measures, including proper encryption, adequate firewalls, and

an adequate protocol for safeguarding Plaintiff and Class Members' Personal Health Information.

255. It was reasonably foreseeable to Commonwealth Health that by installing the Meta Pixel on its websites that patients' and potential patients' Personal Health Information would be transmitted to Facebook without their knowledge or consent. And, in fact, this was the purpose behind Commonwealth Health's installation of the Meta Pixel tool. It was also foreseeable to Commonwealth Health that sharing patients and potential patients' Personal Health Information with third parties without patients' and potential patients' knowledge or consent would result in serious consequences for patients.

256. Commonwealth Health realized or should have realized that installing the Meta Pixel on its websites would result in the transfer of Plaintiff and Class Members' Personal Health Information to third parties, including, but not limited to, Facebook.

257. Commonwealth Health breached its duty of reasonable care in collecting and storing their personal information by disclosing Personal Health Information about Plaintiff and Class Members, including their status as patients, the content of their communications, and information about their doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment to third parties.

258. Commonwealth Health's breach caused Plaintiff and Class Members damages, including but not limited to, the following:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Commonwealth Health eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Commonwealth Health took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members'

knowledge, consent, or authorization and without sharing the benefit of such value;

- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Commonwealth Health's duty to maintain the confidentiality of their Personal Health Information; and
- f. Commonwealth Health's actions diminished the value of Plaintiff and Class Members' personal information.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Commonwealth Health in excess of \$1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

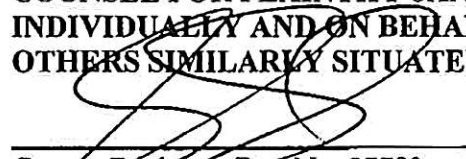
PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, asks for judgment in his favor, and that the Court enter an order as follows:

- a. Certifying the Class and appointing Plaintiff as the Class's representative;
- b. Appoint the law firms of Bochetto & Lentz, P.C., Turke & Strauss, LLP, and Ahmad, Zavitsanos, & Mensing P.C. as class counsel;
- c. Finding that Commonwealth Health's conduct as alleged herein was unlawful;
- d. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Commonwealth Health from making any further disclosure of Plaintiff or Class Members' communications to third parties without the Plaintiff or Class Members' express, informed, and written consent;
- e. Awarding statutory damages of \$1,000 per Plaintiff and Class Members pursuant to 18 Pa. C.S.A. § 5725(a)(1);

- f. Imposing a constructive trust against Commonwealth Health through which Plaintiff and Class Members can be compensated for any unjust enrichment gained by Commonwealth Health;
- g. Awarding damages for violations of Plaintiff and Class Members' right to privacy;
- h. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- i. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;
- j. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;
- k. Awarding costs of suit; and
- l. Such other and further relief to which Plaintiff and Class Members may be entitled.

**RESPECTFULLY SUBMITTED,
COUNSEL FOR PLAINTIFF JANE DOE,
INDIVIDUALLY AND ON BEHALF OF ALL
OTHERS SIMILARLY SITUATED**



George Bochetto, Bar. No. 27783
David P. Heim, Bar. No. 84323
John A. O'Connell, Bar. No. 205527
BOCHETTO & LENTZ, P.C.
1524 Locust St.
Philadelphia, PA 19102
Tel: (215) 735-3900

Foster C. Johnson (*pro hac vice forthcoming*)
David Warden (*pro hac vice forthcoming*)
Weining Bai (*pro hac vice forthcoming*)
AHMAD, ZAVITSANOS, & MENSING, PLLC
1221 McKinney Street, Suite 3460
Houston, Texas 77010
(713) 655-1101

Samuel J. Strauss (*pro hac vice forthcoming*)
Raina C. Borrelli (*pro hac vice forthcoming*)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775

Dated: January 19, 2023

VERIFICATION

I, [REDACTED], hereby certify that I have read the foregoing and that the following is correct:

The facts set forth in the foregoing document are based upon information which I have furnished to counsel, as well as upon information which has been gathered by counsel and or/others acting on my behalf in this matter. The language of the document is that of counsel and not my own. I have read the document, and to the extent it is based upon information which I have given counsel, it is true and correct to the best of my knowledge, information and belief. To the extent the content of the document is that of counsel, I have relied upon such counsel in making this Verification. I hereby acknowledge that the facts set forth in the aforesaid document are made subject to the penalties of 18 Pa. C.S.A. §4904 relating to unsworn falsification to authorities.

Date: January 19, 2023

[REDACTED]